Erstellen eines Schlüssel Paares für CAcert

Um selber ein Schlüssel Paar zu erzeugen, benötigen Sie das Programm OpenSSL. Laden Sie es sich von der OpenSSL Webseite und installieren Sie es.

Sobald Sie die Installation abgeschlossen haben, können Sie sich mit dem folgenden Befehl auf der Kommandozeile ein Schlüsselpaar generieren:

```
openssl genrsa -aes256 -out cacert.org.privatekey.pem 4096
```

Damit generieren Sie sich ein RSA Schlüssel Paar mit einer Länge von 4096 Bit. Gespeichert wird dies in der Datei cacert.org.privatekey.pem. Diese müssen Sie unbedingt sicher aufbewahren! Beim Erstellen werden Sie nach einem Passwort zum Schutz der Datei gefragt. Geben Sie hier ein möglichst starkes Passwort an (möglichst lang, Klein- und Großbuchstaben, Zahlen und Sonderzeichen).

Anschliessend erstellen Sie die Zertifizierungs-Anfrage (CSR) mit dem folgenden Befehl:

```
openssl req -new -x509 -key cacert.org.privatekey.pem -out cacert.org.csr -
days 7
```

Damit stellen Sie einen Antrag für ein X.509 Zertifikat, den Sie anschliessend nurnoch an CAcert übermitteln müssen. Dieser Antrag ist 7 Tage gültig. Er ist in der Datei cacert.org.csr gespeichert. Der Inhalt dieser Datei muss in das Textfeld Wahlweise Client-CSR in dem CAcert Formular kopiert werden.

Wenn Sie nun das Formular abschicken, bekommen Sie diesmal keine PKCS12-Datei zum Download bzw. zur Installation angeboten, sondern es wird Ihnen Ihr ausgestelltes Zertifikat als Text (im PEM Format) angezeigt. Diesen Text kopieren Sie sich in eine Datei namens publiccert.pem.

Um den Inhalt des gerade erhaltenen (öffentlichen) Zertifikats zu überprüfen, können Sie den folgenden Befehl eingeben:

```
openssl x509 -in publiccert.pem -noout -text
```

Jetzt müssen Sie sich nurnoch eine eigene PKCS12-Datei erstellen. Sie fügen das gerade erhaltene Zertifikat im PEM Format sowie Ihren privaten Schlüssel in der Datei zusammen. Diese Datei wird Ihr privates Zertifikat Sein und Sie müssen es dementsprechend sicher aufbewahren! Der Befehl um die PKCS12-Datei zu erzeugen, lautet wie folgt:

```
openssl pkcs12 -des3 -export -in publiccert.pem -inkey
cacert.org.privatekey.pem -out privatecert.p12
```

Die resultierende Datei privatecert.p12 können Sie nun in Ihren Webbrowser, E-Mail Client oder eine andere Software die X.509 Zertifikate verwendet importieren.

Quellen

- http://sachse.info/cacert.html